(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 594**

(51) Int. CI.:
H04W 8/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08844578 .8**
(96) Fecha de presentación: **27.10.2008**
(97) Número de publicación de la solicitud: **2218270**
(97) Fecha de publicación de la solicitud: **18.08.2010**

(54) Título: **SISTEMA Y PROCEDIMIENTO PARA LA AUTENTICACIÓN DE UNA TRANSFERENCIA DE CONTEXTO.**

(30) Prioridad:
29.10.2007 US 983450 P

(45) Fecha de publicación de la mención BOPI:
02.03.2012

(45) Fecha de la publicación del folleto de la patente:
02.03.2012

(73) Titular/es:
NOKIA CORPORATION
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:
BLOMMAERT, Marc;
FORSBERG, Dan;
MADEMANN, Frank y
NIEMI, Valtteri

(74) Agente: **López Bravo, Joaquín Ramón**

DESCRIPCIÓN

Sistema y procedimiento para la autenticación de una transferencia de contexto.

Referencia cruzada a solicitudes relacionadas

La presente solicitud reivindica el beneficio de la Solicitud Provisional de los Estados Unidos Nº de Serie 60/983.450, presentada el 29 de Octubre de 2007, y titulada "Sistema y Procedimiento para la Autenticación de una Transferencia de Contexto desde una MME hacia el Sistema de 3GPP Heredado."

Antecedentes

Esta sección pretende proporcionar los antecedentes para el material que se describe más adelante y/o se define en las reivindicaciones. Esta sección de antecedentes puede incluir conceptos que podrían seguirse pero que no son necesariamente los que se han concebido o seguido anteriormente. A menos que se indique otra cosa específicamente, esta sección no es la técnica anterior a la descripción y reivindicaciones en esta solicitud y no se admite nada en esta sección que sea técnica anterior.

En la Red de Acceso de Radio Terrestre (UTRAN) del Sistema de Telecomunicaciones Móviles Universal (UMTS), se usa una firma del identificador de la estación móvil temporal de la red de paquetes conmutados (P-TMSI) para autenticar y autorizar la transferencia de la información de contexto del equipo de usuario (UE). Como se entiende generalmente en la técnica, la información de contexto del protocolo de paquetes de datos (PDP) para el UE es un registro de valores de parámetros que proporciona información necesaria para establecer una conexión. Estos parámetros pueden incluir información acerca del tipo de contexto del PDP que se está usando, la información de la Calidad de Servicio (QoS), etc. La autenticación y la autorización se realizan cuando se transfiere la información de contexto del UE entre entidades de red de un sistema único, o entre entidades de red de diferentes sistemas, cuando cambia el nodo de soporte (SGSN) del Servicio de Radio General de Paquetes (GPRS). Tal cambio puede producirse cuando el UE se está transfiriendo debido al movimiento a una localización diferente. De este modo, el SGSN antiguo (es decir, el SGSN desde el cual se está transfiriendo el UE) puede verificar que la petición de transferencia de contexto desde un nuevo SGSN (es decir el SGSN al cual se está transfiriendo el UE, también llamado SGSN cesionario) es válida y se refiere al UE identificado en la petición de transferencia de contexto. La señalización salto por salto entre elementos de red puede estar protegida por la seguridad del dominio de red (NDS) de modo que ningún intruso pueda modificar los paquetes.

Los mecanismos para la autenticación de las peticiones de transferencia de la información de contexto en un sistema del Proyecto de Miembros de la 3ª Generación (3GPP) Evolucionado son diferentes de los sistemas UMTS y GPRS heredados. En un sistema de 3GPP evolucionado (también conocido como UTRAN Evolucionada (E-UTRAN) o de Evolución a Largo Plazo (LTE)), que se trata por ejemplo en la Especificación Técnica del 3GPP (TS) 23.401, no se espera que se use la firma del P-TMSI. En cambio, la asociación del nivel de seguridad del estrato de no acceso (NAS) y las claves correspondientes y los valores COUNT se gestionan durante del modo de reposo (IDLE). Toda la señalización a nivel NAS se autentica, por la protección de integridad, con las claves NAS. Como se describe en el documento TS 23.401 y como es conocido en la técnica, la movilidad del UE en una red 3GPP evolucionada se controla por un elemento conocido como la Entidad de Gestión de Movilidad (MME). Las funcionas de una MME pueden incluir la señalización NAS, la Gestión de Movilidad (MM), la señalización de seguridad NAS, y la autenticación. Durante la movilidad desde una MME antigua a una MME nueva, la MME antigua autentica una petición de transferencia de contexto y la señalización de movilidad basada en una Muestra_NAS calculada con una clave de protección de integridad.

Cuando un UE se mueve entre el UMTS, el Sistema Global para Comunicaciones Móviles (GSM) o el GPRS y un sistema 3GPP evolucionado, la transferencia de contexto y la señalización de movilidad deben seguir autenticándose. Sin embargo, hay un problema con respecto a cómo autoriza el sistema 3GPP evolucionado las peticiones de transferencia de contexto o la señalización de movilidad que vienen desde un sistema UMTS/GPRS que no proporciona los mismos mecanismos de autorización que el sistema 3GPP evolucionado. En particular un nodo cesionario de la red UMTS/GPRS (un nodo dentro del dominio al cual se está transfiriendo el UE) espera una firma del P-TMSI desde un UE (es decir, un terminal móvil u otro dispositivo). El nodo de UMTS/GPRS proporciona a continuación esa firma del P-TMSI a una entidad de red par (por ejemplo, un SGSN desde el cual se está transfiriendo el UE) durante la petición de información de contexto para ese UE. Sin embargo, el sistema 3GPP evolucionado (EPS) no proporciona el manejo de la firma del P-TMSI. En realidad, pueden usarse partes del elemento de información (IE) que mantienen la firma del P-TMSI en un mensaje de señalización del sistema UTRAN para un propósito diferente en un sistema 3GPP evolucionado. Por ejemplo, algunos de los bits de ese IE pueden ser necesarios en un sistema 3GPP evolucionado para mantener las partes del Sistema de Paquetes Evolucionado TMSI (S-TMSI). Esto reduce los bits disponibles para el uso del material de autenticación para la autorización de la transferencia de contexto. La arquitectura WG2 SA TSG del 3GPP – documento S2 Nº58 titulado: "Procedimiento RAU de la MME/SGW para el SGSN pre-versión-8" desvela una petición de transferencia de contexto entre dos entidades de red que pertenecen a sistemas diferentes.

Sumario

Este sumario se proporciona para introducir una selección de conceptos en una forma simplificada que se describen además más adelante en la Descripción Detallada. Este Sumario no pretende identificar las características claves o las características esenciales de la invención.

De acuerdo con al menos algunas realizaciones, un equipo de usuario (UE) y una MME en un sistema 3GPP evolucionado genera cada uno material de autenticación. Ese material de autenticación puede transportarse in el interior del campo de la firma del P-TMSI de un mensaje de señalización de UMTS desde el UE al SGSN de UMTS/GPRS cuando el UE se está transfiriendo a un sistema UTRAN/GERAN. Ese material de autenticación también puede comunicarse desde el SGSN del UMTS/GPRS a la MME (del sistema 3GPP evolucionado) desde el cual se está transfiriendo el UE. En esta disposición, la MME antigua puede autenticar a continuación la petición de transferencia de contexto desde el sistema 3GPP legado en base al material de autenticación transferido y el conocimiento de cómo se crea el material de autenticación.

En al menos algunas realizaciones, la MME y el UE deducen el material de autenticación en base a las claves específicas del usuario. El material de autenticación, que puede deducirse cuando se crean las claves NAS o bajo demanda, pueden incorporarse a continuación en el contenido del campo de la firma del P-TMSI para la señalización del 3GPP heredado desde el UE y desde el SGSN del UMTS/GPRS a la MME. En el caso de que se usen una o más claves NAS (o se usen claves derivadas de las claves NAS), el material de autenticación generado puede cambiarse cada vez que cambian las claves NAS. De este modo no se necesita transferir el número de secuencia dentro del campo de la firma del P-TMSI, proporcionando de este modo una seguridad mejorada bajo restricciones de una longitud determinada del campo de la firma del P-TMSI reutilizado. Si las claves NAS cambian cada vez que se mueve el UE, por ejemplo, desde la UTRAN a la E-UTRAN, el material de autenticación también se refrescará cuando el UE se mueve de vuelta a la UTRAN.

Con las diversas realizaciones descritas en este documento, no se necesita ningún mecanismo similar a la firma del P-TMSI para el sistema de 3GPP evolucionado, es decir, no hay ninguna necesidad de crear una firma del P-TMSI en la MME antes de recibir una petición de autenticación de la transferencia de contexto. Tampoco hay ninguna necesidad de transferir una muestra o una firma desde la MME al UE. El UE puede generar material de autenticación (por ejemplo, una muestra) bajo demanda, evitando por lo tanto los requisitos de almacenamiento para la muestra. Esa muestra puede transportarse en los mensajes de señalización de UMTS existentes.

Estas y otras ventajas y características, junto con la organización y el modo de operación de las mismas, se hará evidente a partir de la siguiente descripción detallada cuando se toma en conjunción con los dibujos adjuntos en los que elementos iguales tienen las mismas referencias numéricas a través de los diversos dibujos descritos más adelante.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques de una arquitectura de itinerancia para la interoperación entre las versiones de las normativas iniciales y las versiones del 3GPP evolucionadas de acuerdo con al menos algunas realizaciones.

La Figura 2 es un diagrama que muestra los intercambios de señales en una MME para un procedimiento de actualización del área de itinerancia del SGSN de acuerdo con al menos algunas realizaciones.

La Figura 3 es una vista en perspectiva de un dispositivo electrónico que puede usarse en conjunción con una implementación de al menos algunas realizaciones.

La Figura 4 es una representación esquemática de la circuitería que puede incluirse en el dispositivo electrónico de la Figura 3.

La Figura 5 es un diagrama de bloques de la MME mostrada en la Figura 2.

Descripción detallada

En al menos algunas realizaciones un equipo de usuario (UE) y una Entidad de Gestión de Movilidad (MME) en un sistema de 3GPP evolucionado generan cada uno un material de autenticación (por ejemplo, una muestra). El material de autenticación puede transportarse en el interior de un campo de la firma del P-TMSI de un mensaje de señalización del UMTS heredado desde el UE al SGSN del UMTS/GPRS en una UTRAN o en una Red de Acceso de Radio de Borde (GERAN) / GSM dentro de la cual se está transfiriendo el UE. Por ejemplo, el UE puede que no esté al tanto de si se transfiere dentro del dominio de una MME del 3GPP evolucionado o dentro del dominio de un SGSN en una UTRAN o GERAN heredada, y de este modo el UE puede usar la señalización heredada para la señalización UE-SGSN de la RAU (Actualización del Área de Encaminamiento). El material de autenticación también puede usarse en un mensaje de señalización desde el SGSN del UMTS/GPRS a la antigua MME del sistema de 3GPP evolucionado desde el cual se transfiere el UE. En esta disposición, el UE crea el material de autenticación y lo proporciona al SGSN, con el SGSN proporcionando a continuación ese material de autenticación a la MME antigua en una petición de transferencia de contexto. La MME antigua, con el conocimiento de cómo se creó el

material de autenticación en el UE, puede recrear a continuación el material de autenticación una vez recibida la petición de transferencia de contexto que identifica el UE y autentica la petición de transferencia de contexto.

En algunas realizaciones, la MME y el UE deducen el material de autenticación en base a al menos una clave específica del usuario (por ejemplo, la K_ASME, K_NASInt, o K_NASenc). El material de autenticación puede deducirse cuando se crean las claves del estrato de no acceso (NAS) o bajo demanda. Si se usan una o más claves NAS (o si se usan una o más claves deducidas de las claves NAS), el material de autenticación generado puede cambiarse cada vez que cambian las claves NAS. Por lo tanto, no tienen que transferirse un número de secuencia dentro del campo de la firma del P-TMSI, lo que proporciona una seguridad mejorada bajo las restricciones de longitud determinada del campo de firma del P-TMSI reutilizado. Si las claves NAS cambian cada vez que se mueve el UE, por ejemplo desde la UTRAN a la E-UTRAN, el material de autenticación también se refrescará cuando el UE se mueve de vuelta a la UTRAN. Si se usa la clave específica del usuario de más alto nivel (por ejemplo, K_ASME), el material de autenticación puede basarse en el valor existente del número de secuencia en aumento actual, tal como el valor COUNT de señalización del estrato no acceso (NAS) del enlace descendente o el enlace ascendente. COUNT es un número de secuencia de paquetes en aumento. Los valores de COUNT se almacenan en memoria. Pueden almacenarse en la memoria sólo algunos de los bits más altos del valor COUNT y el resto de bits pueden señalizarse sobre los mensajes. Cada vez que hay una señalización NAS, los valores de COUNT se actualizan y de este modo el material de autenticación también se refresca.

Con las diversas realizaciones descritas en este documento, no se necesita ningún mecanismo similar a la firma del P-TMSI para el sistema de 3GPP evolucionado, y no hay ninguna necesidad de transferir una firma del P-TMSI (ni ningún otro tipo de muestra o firma) desde la MME al UE o para crear el material de autenticación antes de la recepción de una petición de autenticación desde un SGSN cesionario. El equipo de usuario también puede generar una muestra a demanda, significado que no hay ningún requisito de almacenamiento para la muestra. Es más, con diversas realizaciones, los mensajes de señalización de UMTS existentes pueden usarse para transportar el material de autenticación (por ejemplo, la muestra).

La Figura 1 es un diagrama de bloques de una arquitectura de itinerancia para la interoperación entre las versiones de normativas de 3GPP inicial y evolucionada de acuerdo con al menos algunas realizaciones. Como se muestra en la Figura 1, el UE 100 interactúa con una red de UTRAN Evolucionada (E-UTRAN) 110, que a su vez se puede comunicar tanto con una puerta de enlace en servicio (SGW) 120 como con la MME 130. Además de la comunicación con la SGW 120 directamente, la MME 130 también puede comunicar con un SGSN 140, que está conectado tanto a una UTRAN como a una GERAN 160. Tanto la MME 130 como el SGSN 140 también interactúan con un servidor de abonado local (HSS) 170. Tanto el SGSN 140 como la SGW 120 comunican con una puerta de enlace (PGW) 180 de la red de datos privada (PDN), que a su vez comunica tanto con una función de política de normas de cargo (PCRF) 190 como los propios servicios de IP del operador 195.

La Figura 2 es un diagrama que muestra los intercambios de señales en una MME para el procedimiento de actualización del área de encaminamiento del SGSN de acuerdo con al menos algunas realizaciones. En ciertas realizaciones, los mensajes desde y hacia al SGSN, así como los elementos de información contenidos en los mismos, son los mismos que los especificados en la Especificación Técnica del 3GPP (TS) 23.060 para el procedimiento de actualización del área de encaminamiento del SGSN. Los mensajes desde y hacia la MME 130 o la SGW 120, así como los elementos de información contenidos en los mismos, son los mismos que los especificados en esta especificación técnica para el procedimiento de actualización del área de encaminamiento inter RAT (Tecnología de Acceso de Radio).

Refiriéndonos a la Figura 2, el procedimiento de actualización del área de encaminamiento de la MME al SGSN comienza en 200, donde el UE 100 envía una "petición de actualización del área de encaminamiento" al nuevo SGSN 140. La petición de actualización del área de encaminamiento incluye información tal como la identificación del área de encaminamiento antiguo (RAI), una Muestra_NAS (un código de autenticación del estrato no de acceso, que es el material de autenticación calculado por el UE y que sirve como la firma de P-TMSI "antigua"), el tipo de actualización, la marca de clase, los parámetros de recepción discontinua (DRX) y la información de la capacidad de la red del UE. El subsistema de la estación base del sistema (BSS) añade la identidad global de la célula incluyendo el grupo de aplicación real (RAC) y el código del área de localización (LAC) de la célula donde se recibió el mensaje antes de pasar el mensaje al nuevo SGSN 140. La marca de clase contiene las capacidades multi-ranura del GPRS del UE y los algoritmos de cifrado del GPRS soportados, como se define en el documento TS 24.008. Los parámetros DRX indican si el UE usa o no la recepción discontinua, y si es así, la longitud de ciclo de DRX. El UE 100 indica una de las identidades del área de seguimiento registrado (TAI) y la antigua RAI y calcula la Muestra_NAS como la firma P-TPMSI antigua en base a K-NASInt (una clave de integridad NAS específica de un usuario) o K_ASME (clave de la Entidad de Gestión de Seguridad de Acceso, una clave raíz almacenada en la MME y el UE después de una autenticación satisfactoria) y el valor respectivo de COUNT (y el contador incremental) de la NAS respectivo del enlace ascendente o el enlace descendente.

En 205, en la Figura 2, el nuevo SGSN 140 envía una "petición de contexto de SGSN" a la MME antigua 130 para obtener la gestión de movilidad (MM) y los contextos del protocolo de paquetes de datos (PDP) para el UE. La petición de contexto del SGSN incluye la antigua RAI, una identidad del enlace lógico temporal (TLLI) y/o el P-TMSI, la firma del P-TMSI antigua, y las nuevas direcciones del SGSN. Como se explica más adelante, la antigua MME

130 puede enviar a continuación una "respuesta del contexto del SGSN" en 210 de vuelta al nuevo SGSN 140.

El SGSN puede dirigir la petición de contexto del SGSN a la MME de diversas formas. Si el nuevo SGSN proporciona funcionalidad para la conexión intra-dominio de los nodos de la red de acceso de radio (RAN) a los nodos de la red central múltiple (CN), el nuevo SGSN puede deducir la antigua MME a partir de la RAI antigua y el P-TMSI antiguo (o TLLI) y enviar el mensaje de petición de contexto del SGSN a esta MME antigua. De lo contrario, el nuevo SGSN deduce la MME antigua a partir de la antigua RAI. El nuevo SGSN 140 deduce la MME que cree que es la antigua MME 130. Esta MME deducida es propiamente la antigua MME 130, o está asociada con la misma área de pila que la MME antigua real. Una MME deducida que no es la MME antigua determina la MME antigua correcta 130 a partir del P-TMSI (o TLLI) y retransmite el mensaje a la MME antigua real 130.

Una vez recibida la petición de contexto del SGSN, la MME antigua 130 valida el valor de la firma antigua del P-TMSI, que está en la Muestra_NAS calculada por el equipo del usuario, en base a K_ASME y los valores respectivos de COUNT del enlace descendente de la NAS (que son conocidos para la MME 130). En el caso de que la MME tenga múltiples claves K_ASME identificadas con diferentes Identificadores del Conjunto de Claves (KSI), por ejemplo debido a un procedimiento de Autenticación y Acuerdo de Claves (AKA) que acaba de producirse, la MME puede calcular la muestra de autenticación con todas las claves disponibles para determinar si una de las claves disponibles es una coincidencia. La MME antigua también puede calcular y proporcionar la muestra al nuevo SGSN. Sin embargo, por razones de protección de repetición, si el valor de COUNT se usa como un parámetro en la generación de muestras de autenticación, se reutiliza, es decir, se aumenta. La KSI también puede transferirse dentro del campo de la firma del P-TMSI, particularmente en el caso de la opción de firma del P-TMSI de longitud variable. El valor de COUNT puede que no está sincronizado entre el UE y la MME debido a las pérdidas de mensajes de señalización de NAS, de este modo, la MME puede calcular la muestra de autenticación con varios valores de COUNT dentro del intervalo del valor de COUNT actual (por ejemplo, [COUNT-L del enlace descendente de NAS actual, COUNT del enlace descendente de NAS actual]).

Si la firma del P-TMSI antigua es válida, entonces la MME antigua 130 responde con la "respuesta de contexto de SGSN". El mensaje de respuesta del contexto del SGSN incluye información tal como el contexto de la MM, los contextos de PDP, el servicio de encaminamiento de la red (NRS), y el contexto de seguridad.

Si el valor calculado por la MME antigua 130 en base al número de secuencia de NAS recibido y la antigua K_ASME almacenada no coinciden con la Muestra_NAS recibida desde el SGSN, la MME 130 responde con la causa de error apropiada. Esto puede iniciar las funciones de seguridad en el nuevo SGSN 140. Si esas funciones de seguridad en el SGSN 140 autentican al UE 100 correctamente, entonces el nuevo SGSN 140 envía otro mensaje de petición de contexto del SGSN (la RAI antigua, la TLLI, el equipo de usuario / estación móvil validada, la dirección del nuevo SGSN) a la MME antigua 130 indicando que el nuevo SGSN 140 ha autenticado al UE 100. Si el nuevo SGSN 140 indica que ha autenticado al UE 100, entonces la MME antigua 130 responde con la "respuesta de contexto del SGSN" como se ha descrito anteriormente.

Una vez enviado un mensaje de respuesta del contexto de SGSN, la MME antigua 130 almacena la dirección del nuevo SGSN 140 de modo que permite a la antigua estación base (eNB) de la red de acceso de radio terrestre universal, la puerta de enlace en servicio (SGW) 120 o a otras entidades redirigir los paquetes de datos al nuevo SGSN 140. La MME antigua 130 comienza a continuación un temporizador, el propósito del cual se trata más adelante. La MME mapea la información de la portadora del Sistema de Paquetes Evolucionado (EPS) al contexto de PDP. También se determina si realizar y cómo realizar la retransmisión de datos desde la eNB 155 o la SGW 120 al SGSN.

Una vez recibida la respuesta de contexto del SGSN, el nuevo SGSN 140 ignora la capacidad de la red del UE 100 contenida en el contexto de la MM de la respuesta de contexto del SGSN sólo si el SGSN 140 ha recibido anteriormente una capacidad de la red del UE en la petición de actualización del área de encaminamiento. El servicio de encaminamiento de la red (NRS) en la respuesta de contexto del SGSN indica el soporte del UE 100 del control de la portadora solicitado de la red para el nuevo SGSN 140. El contexto de seguridad en la repuesta de contexto del SGSN incluye el identificador del conjunto de claves (KSI) y la clave de cifrado de la UTRAN (CK) / la clave de integridad (IK) deducida de la K_ASME (la clave de la entidad de gestión de seguridad de acceso). Los vectores de autenticación de UMTS también pueden incluirse. Los vectores de autenticación de la E-UTRAN no se transfieren hacia fuera del la E-UTRAN, y de este modo no se incluyen en la respuesta de contexto del SGSN.

En 215 en la Figura 2, pueden ejecutarse diversas funciones de seguridad. Tales procedimientos se tratan, por ejemplo, en la sección de "Funciones de Seguridad" del documento TS 23.060 del 3GPP. Si se soporta el modo de cifrado, el modo de cifrado se fija en este punto. Si el mensaje de respuesta de contexto del SGSN transmitido anteriormente en 210 no incluyó una identidad internacional del equipo de la estación móvil y el número de versión software (IMEISV), y si se soporta la detección automática del dispositivo (ADD) por el SGSN, a continuación el SGSN también puede recuperar el IMEISV del UE 100 en este punto. Si las funciones de seguridad fallan, por ejemplo debido a que el SGSN no puede determinar la dirección del registro de localización local (HLR) para establecer el diálogo de "Envío de la Información de Autenticación", a continuación se devuelve un mensaje de rechazo al equipo de usuario 100, notificando la causa apropiada.

En 220 en la Figura 2, el nuevo SGSN 140 envía un mensaje de "confirmación del contexto del SGSN" a la MME antigua 130. En este punto la MME antigua 130 marca, en su información de contexto, que la información en las puertas de enlace y el HSS 170 son inválidas. Esto activa la SGW 120, la puerta de enlace PDN 180 y el HSS 170 para que se actualicen si el UE 100 inicia un procedimiento de actualización del área de seguimiento de vuelta a la MME antigua 130 antes de completar el procedimiento de actualización del área de encaminamiento en funcionamiento. Si las funciones de seguridad no autentican al UE 100 correctamente, a continuación la petición de actualización del área de encaminamiento se rechaza y el nuevo SGSN 140 envía una indicación de rechazo a la MME antigua 130. La MME antigua 130 continuaría entonces como si la petición de contexto del SGSN 205 nunca se hubiera recibido.

Si el UE 100 se autentica correctamente, sin embargo, también se determina si el MME antiguo 130 se informa de que el nuevo SGSN 140 está listo para recibir los paquetes de datos que pertenecen a los contextos de PDP activados y cómo realizar cualesquiera retransmisión de datos desde la eNB 155 o la SGW 120 al nuevo SGSN 140. En el caso de que el UE 100 esté en un estado LTE_Activo en la MME antigua 130, a continuación en 225, la MME antigua 130 envía un mensaje "comando de retransmisión de datos " al eNB 155. El comando de retransmisión de datos incluye información tal como la portadora del acceso de radio (RAB_ID), la dirección de la capa de transporte, y la información de la asociación de transporte S1.

En 230 en la Figura 2, la eNB antigua 155 duplica las unidades del protocolo de red almacenadas (N-PDU) y comienza a encapsularlas hacia el nuevo SGSN 140. Las N-PDU adicionales recibidas desde la SGW 120 antes de que expire el temporizador de la MME 130 (descrito anteriormente) también se duplican y se encapsulan hacia el nuevo SGSN 140. Ninguna N-PDU se retransmiten al nuevo SGSN 140 después de la expiración del temporizador.

En 235, el nuevo SGSN 140 envía una "petición de actualizar contexto de PDP" a la PGW respectiva 180. La petición de actualizar contexto de PDP incluye información tal como la dirección del nuevo SGSN 140, el Identificador del Punto de Extremo del Túnel (TEID), la información concerniente a la calidad de servicio negociada (QoS), la identidad de la red en servicio, la interfaz de la puerta de enlace común (CGI) / la información de la interfaz del área en servicio (SAI), el tipo de RAT, un indicador de disponibilidad de recursos (RAI) CGI / SAI una indicación de soporte de cambios, y la información de NRS.

El nuevo SGSN 140 envía la identidad de la red en servicio a la PGW 180. El NRS indica al SGSN el soporte del control de la portadora de red solicitada. El nuevo SGSN 140 indica que soporta el procedimiento y, si lo soporta, indica que el UE 100 también lo soporta en el mensaje de respuesta del contexto del SGSN 210 tratado anteriormente. Si el NRS no está incluido en el mensaje de petición de actualizar el contexto de PDP 235, la PGW 180, siguiendo este procedimiento, realiza una modificación del contexto de PDP iniciada por el SGSN para cambiar el modo de control de la portadora (BCM) a 'Solo MS' para todas las direcciones del PDP / pares APN para los cuales para los cuales el BCM actual es 'sólo NW'.

Las PGW 180 actualizan sus campos de contexto de PDP y devuelven una "respuesta de actualización del contexto de PDP" en 240. La respuesta de actualización del contexto de PDP incluye información tal como el TEID, información de compresión de la carga útil prohibida, información de restricción de Nombre del Punto de Acceso (APN), y la información respecto a si se requiere una información de cambio de CGI/SAI/RAI. La información de prohibición de compresión de la carga útil indica que el SGSN 140 debería negociar la ausencia de compresión de datos para el contexto de PDP.

En 245 en la Figura 2, el nuevo SGSN 140 informa al Registro de Localización Local (HLR) en el HSS 170 del cambio de SGSN enviando información de "actualizar localización". Esta información puede incluir el número del SGSN, la dirección del SGSN, la identidad internacional del abonado móvil (IMSI), y la IMEISV. La IMEISV se envía si se soporta la función ADD.

En 250, el HLR en el HSS 170 envía una instrucción de "cancelar localización" a la MME antigua 130. Este mensaje puede incluir información tal como la IMSI y el tipo de cancelación. En este mensaje, el tipo de cancelación se fija a "Actualizar Procedimiento". En el caso de que el temporizador de la MME 130 descrito anteriormente no esté corriendo, entonces la MME antigua 130 elimina los contextos de la MM y la portadora de EPS. De lo contrario, los contextos se eliminan sólo cuando expira el temporizador. La vieja MME 130 también asegura que los contextos de la MM y el PDP se mantienen en la MME antigua 130, en el caso de que el UE 100 inicie otra actualización del área de encaminamiento del SGSN antes de completar la actualización del área de encaminamiento en funcionamiento para el nuevo SGSN 140. La MME antigua 130 confirma la instrucción de cancelar localización 250 con un "Confirmación de cancelar localización", incluyendo la IMSI, en 255. También se determina si la MME antigua 130 o la eNB 155 necesitan completar la retransmisión de cualesquiera N-PDU.

En 260, el HLR en el HSS 170 envía un mensaje de "insertar datos de abonado" al nuevo SGSN 140. Este mensaje incluye la IMSI, y los datos de suscripción de GPRS. El nuevo SGSN 140 valida la presencia del UE 100 en la nueva área de encaminamiento (RA). Si, debido a las restricciones regionales de suscripción o las restricciones de acceso, el UE no tiene permitido agregarse en la RA, entonces el nuevo SGSN 140 rechaza la petición de actualización del área de encaminamiento con una causa apropiada. El nuevo SGSN 140 también puede devolver un mensaje de "Confirmación de inserción de datos de usuario" (incluyendo la IMSI y la información de "área restringida del SGSN")

al HLR en 265. Si todas las comprobaciones son satisfactorias, a continuación el SGSN construye un contexto de la MM para el UE 100 y devuelve un mensaje de "confirmación de inserción de datos de abonado" al HLR (también representado en 265), incluyendo el mensaje la IMSI. En 270 en la Figura 2, el HLR en el HSS 170 confirma el mensaje de "actualizar localización" enviando un mensaje "Confirmación actualización localización", incluyendo la IMSI, al nuevo SGSN 140.

Después de lo anterior, el nuevo SGSN 140 valida la presencia del UE 100 en la nueva RA. Si, debido a las restricciones de itinerancia o las restricciones de acceso, el UE 100 no tiene permitido agregarse en el nuevo SGSN 140, o si falla la comprobación de suscripción, a continuación el nuevo SGSN 140 rechaza la actualización del área de encaminamiento con la causa apropiada. Si todas las comprobaciones son satisfactorias, a continuación el nuevo SGSN 140 construye los contextos de la MM y el PDP para el equipo de usuario. Se establece un enlace lógico entre el nuevo SGSN 140 y el UE 100. El nuevo SGSN 140 responde a continuación al UE 100 con un mensaje "aceptar actualización del área de encaminamiento" en 275, incluyendo un nuevo P-TMSI, una nueva firma del P-TMSI, y un número de recepción de N-PDU. También se determina si se usan números de N-PDU y cómo se usan. Por ejemplo, la recepción del número de N-PDU incluye las confirmaciones para cada uno los identificadores de los puntos de acceso al servicio de la capa de red de modo confirmado (NSAPI) usados por el UE 100, confirmando por lo tanto que todas las N-PDU originadas por el móvil se transfieren satisfactoriamente antes del comienzo del procedimiento de actualización.

En 280 en la Figura 2, el UE 100 confirma el nuevo P-TMSI devolviendo un mensaje de "actualización del área de encaminamiento completa", incluyendo el número de N-PDU de recepción, al nuevo SGSN 140. En este instante, el control del enlace lógico (LLC) y el protocolo de convergencia dependiente de la subred (SNDCP) en el UE 100 se reinician. Una vez más, se determina también si se usan los números N-PDU y cómo. Por ejemplo, el número de N-PDU recibido contiene las confirmaciones para cada uno de los NSAPI del modo confirmado usados por el UE 100, confirmando por lo tanto que todas las N-PDU terminadas en móvil se transfieren satisfactoriamente antes del comienzo del procedimiento de actualización. Si el número de N-PDU recibido confirma la recepción de las N-PDU que se retransmitieron desde la MME antigua 130, a continuación estas N-PDU pueden descartarse por el nuevo SGSN 140. Cuando el temporizador en la MME 130 tratado anteriormente expira, la MME antigua 130 libera cualesquiera recursos de la eNB y la SGW (no mostrados).

En el caso de una operación de actualización del área de encaminamiento rechazado, debido a la suscripción regional, las restricciones de itinerancia, las restricciones de acceso, o debido a que el SGSN no puede determinar la dirección del HLR para establecer el diálogo de actualización de la localización, a continuación el nuevo SGSN 140 no construye un contexto de MM. Se devuelve un mensaje de rechazo al UE 100 con una identificación de la causa respectiva. El UE 100 no reintenta una actualización del área de encaminamiento para esa RA. El valor de RAI se borra cuando el UE 100 se enciende. Si el nuevo SGSN 140 es incapaz de actualizar el contexto de PDP en una o más PGW 180, a continuación el nuevo SGSN 140 desactiva los contextos de PDP correspondientes. Sin embargo esto no debería causar que el SGSN rechace la actualización del área de encaminamiento.

Los contextos de PDP se envían desde la MME antigua 130 al nuevo SGSN 14 en un orden priorizado, es decir el contexto de PDP más importante se envía primero en el mensaje de respuesta del contexto del SGSN. Debería observarse que el procedimiento de priorización exacto a utilizar puede ser dependiente de la implementación. Sin embargo, en ciertas realizaciones la priorizaciones se basa en la actividad actual. El nuevo SGSN 140 determina la restricción de APN máxima en base a la restricción de APN recibida de cada uno de los contextos de PDP desde la PGW 180 y a continuación almacena el nuevo valor máximo de restricción de APN.

Si el nuevo SGSN 140 no es capaz de soportar el mismo número de contextos PDP activos que los recibidos desde la MME antigua 130, entonces el nuevo SGSN 140 puede usar la priorización enviada por la MME antigua 130 como entrada cuando decide qué contextos de PDP se mantendrán activos y cuales se deberían borrar. En cualquier caso, el nuevo SGSN 140 en primer lugar actualiza todos los contextos en una o más PGW 180 y a continuación desactiva los contextos que no puede mantener. Esto no debería causar que el SGSN rechace la actualización del área de encaminamiento.

Si el temporizador anteriormente descrito en la antigua MME 130 expira, y si no se recibió ningún mensaje de cancelar localización (incluyendo la IMSI) desde el HLR, entonces la MME antigua 130 para de retransmitir las N-PDU al nuevo SGSN 140. Si el procedimiento de actualización del área de encaminamiento falla un número de veces permisible máximo, o si el SGSN 140 devuelve un mensaje de rechazo (Causa) de actualización del área de encaminamiento, entonces el equipo de usuario entra en el estado IDLE (reposo).

También se muestra en la Figura 2 una representación de diversas realizaciones que usan la interacción de las Aplicaciones Adaptadas para la Lógica Mejorada de la Red Móvil (CAMEL). En C1 en la Figura 2, los procedimientos de Desconexión_Contexto_PDP_GPRS_CAMEL, Separar_GPRS_CAMEL y la Notificación_PS_CAMEL se invocan en la antigua MME 130. En particular, el procedimiento de Desconexión_Contexto_PDP_GPRS_CAMEL se llama en primer lugar y se invoca varias veces - una por contexto de PDP. El procedimiento devuelve un "Continuar" como resultado. El procedimiento Separar_GPRS_CAMEL se llama a continuación una vez. Este procedimiento también devuelve un "Continuar" como resultado. Finalmente, el procedimiento de Notificación_PS_CAMEL se llama una vez. De nuevo, el procedimiento devuelve un "Continuar" como resultado.

En C2 en la Figura 2, los procedimientos de Sesión_Actualización_Área_Encaminamiento_GPRS_CAMEL y la Notificación_PS_CAMEL se llaman en el nuevo SGSN 140. En particular, se llama primero al procedimiento Sesión_Actualización_Área_Encaminamiento_GPRS_CAMEL. El procedimiento devuelve un "Continuar" como resultado. El procedimiento Notificación_PS_CAMEL se llama a continuación, devolviendo también un "Continuar" como resultado. En C3 en la Figura 2, se llama al procedimiento de Contexto_Actualización_Área_Encaminamiento_GPRS_CAMEL varias veces – una vez por contexto de PDP – y devuelve un "Continuar" como resultado.

Hay varios enfoques que pueden usarse para generar el material de autenticación que puede incorporarse en el campo de la firma del P-TMSI de acuerdo con las diversas realizaciones. En cada una de las realizaciones tratadas en este documento, se usan las claves NAS o claves derivadas de las mismas, aunque el procedimiento para generar las claves con precisión puede variar. Por lo tanto, debería entenderse que los procedimientos de generación del material de autenticación descritos en este documento son sólo de ejemplo por naturaleza. En los enfoques tratados en este documento, la MME antigua 130 no necesita transferir al material de autenticación hacia el equipo de usuario de antemano, como se hace después de la asignación de la firma del P-TMSI para las transferencias de SGSN/UMTS (SGSN/GSM). Esto es porque en las realizaciones tratadas en este documento, la información de Autenticación está basada en claves específicas de usuario. Esto permite una mejora de la seguridad, ya que la transferencia del enlace descendente del material de autenticación al equipo de usuario puede evitarse.

En una realización particular, se calcula una Muestra basada en las claves NAS sobre algunas o todas las partes del mensaje de la UTRAN. En esta disposición, los elementos de información que se envían al SGSN 140 se retransmiten desde el nuevo SGSN 140 a la MME antigua 130 de modo que la MME antigua 130 puede calcular la Muestra_NAS en base al mensaje recibido (es decir, el código de autenticación en base al UE identificado en el mensaje). En una variante de este procedimiento, los contenidos sobre los cuales se calcula la Muestra_NAS se predefinen, y el mensaje recibido por los puntos de la MME para los valores correctos (la identificación del equipo de usuario por el P-TMSI). En este caso, el número de secuencia NAS (SN) no se transfiere dentro de la firma del (P)-TMSI, pero puede usarse como parámetro de entrada. Esto requiere que el valor SN del nivel NAS también se incluye en el campo de la firma del P-TMSI de modo que la MME 130 puede formar el valor correcto de COUNT como un parámetro de entrada para el cálculo de la Muestra_NAS. El valor de COUNT se usa, como en la protección del mensaje NAS normal, por razonas de protección de repetición.

Lo siguiente son dos variantes de los elementos de información de la firma del P-TMSI. La primera variante es de un tamaño fijo, mientras que la segunda variante es de un tamaño variable. En el caso del tamaño fijo el elemento de información de la firma del P-TMSI, la Muestra_NAS con el número de secuencia de NAS se trunca a la longitud fija de por ejemplo 24 bits (el tamaño del P-TMSI en el elemento de información del tamaño fijo). En el caso del elemento de información de la firma del P-TMSI de tamaño variable, puede usarse la Muestra_NAS global de 32 bits (o más) y el número de secuencia (por ejemplo, 4 bits o más). Puede implementarse el soporte tanto del tamaño fijo como el tamaño variable de las firmas del P-TMSI, cuando se transporta la información de autenticación de transferencia de contexto dentro del mensaje de señalización heredado en el interior del elemento de información de la firma del P-TMSI.

En algunas realizaciones, las claves NAS se usan para crear una muestra de una vez tanto en el equipo de usuario como en la MME. Un ejemplo de muestra de autenticación o una función de derivación de la clave de autenticación es como sigue:

Muestra_NAS = KDF (K-NASInt ‖ K_NASenc ‖ S-TMSI ‖ "muestra de autenticación de E-UTRAN a UTRAN")

En lo anterior, KDF es una función de derivación de claves y K_NASInt y K_NASenc son las claves NAS de integridad y cifrado. El símbolo ‖" denota concatenación, y la cadena de caracteres dentro de las comillas (") es una constante. En un caso alternativo, donde el cambio del S-TMSI es suficiente para refrescar la muestra de autenticación, la derivación es como sigue:

Muestra_NAS = KDF (K-ASME ‖ S-TMSI ‖ "muestra de autenticación de E-UTRAN a UTRAN")

En lo anterior, el S-TMSI es la id temporal como se usa en la MME, y K_ASME es una clave raíz desde la cual se deducen las claves NAS. Las claves NAS se definen en el documento TS.33.abc. En otra realización alternativa más, el valor de COUNT también se toma como un parámetro de entrada, haciendo la función de derivación como sigue:

Muestra_NAS = KDF (K-NASInt ‖ K_NASenc ‖ S-TMSI ‖ COUNT ‖ "muestra de autenticación de E-UTRAN a UTRAN")

o

Muestra_NAS = KDF (K-ASME ‖ S-TMSI ‖ COUNT ‖ "muestra de autenticación de E-UTRAN a UTRAN ")

En la forma más simple no se necesita ni el S-TMSI ni la cadena de caracteres. Esto se ilustra como sigue:

Muestra_NAS = KDF (K-ASME ‖ COUNT)

Todas las deducciones de la Muestra_NAS pueden incluir además un valor constante para diferenciar la deducción de la Muestra-NAS de las otras deducciones.

Lo siguiente es una discusión concerniente al momento de creación de la muestra de autenticación descrita anteriormente. La sincronización de los parámetros de entrada para la creación de la muestra en el equipo de usuario y la MME pueden realizarse, en una realización particular, definiendo los puntos de sincronización. En cada uno de los registros satisfactorios en la MME en esta disposición, la muestra se crea de nuevo usando los parámetros de entrada disponibles y se almacenan en ambos extremos para su reutilización. Como alternativa, la sincronización de los parámetros de entrada para la creación de muestras en el equipo de usuario y la MME pueden realizarse retransmitiendo sobre los últimos parámetros disponibles de las claves NAS, S-TMSI, etc. y copiando con otra posibilidad de reintento en el caso de que los parámetros de entrada se hayan cambiado. Por ejemplo, una actualización de la clave NAS con una nueva clave en EPS justo después de la petición de transferencia a la UTRAN puede causar que la MME calcule una muestra diferente. En esta disposición, se evita el almacenamiento anticipado de muestras.

En las realizaciones tratadas anteriormente, si falla la autenticación de la transferencia de contexto, el comportamiento de la red / señalización debería ser el mismo.

El elemento de información de la firma del P-TMSI definida por el UMTS tiene sólo significado local para el SGSN que lo genera y lo asigna al equipo del usuario. En los sistemas 3GPP evolucionados, tanto el equipo de usuario como la MME calculan la muestra de autenticación. Por lo tanto la MME no tiene que proporcionar una firma similar para el equipo de usuario como en la UTRAN, es decir, no hay ninguna transferencia de la "firma del P-TMSI" al equipo de usuario desde la MME.

El nivel de seguridad de los enfoques descritos anteriormente difiere dependiendo de la implementación particular. En general, cuanto más largo es el material de autenticación, mejor es la protección frente a los ataques de Denegación del Servicio (DoS).

Las Figuras 3 y 4 muestran un dispositivo móvil representativo 12 que puede actuar como un equipo de usuario (UE) con el que pueden implementarse diversas realizaciones. Los dispositivos descritos en este documento pueden incluir cualquiera y/o todas las características descritas en las Figuras 3 y 4. Debería entenderse, sin embargo, que la presente invención no pretende limitarse a un tipo particular de dispositivo electrónico. El dispositivo móvil 12 de las Figuras 3 y 4 incluye una carcasa 30, una pantalla 32 en la forma de una pantalla de cristal líquido, un teclado 34, un micrófono 36, un auricular 38, una batería 40, un puerto de infrarrojos 42, una antena 44, una tarjeta inteligente 46 en la forma de una Tarjeta de Circuito Integrado Universal (UICC) de acuerdo con una realización, un lector de tarjetas 48, una circuitería de la interfaz de radio 52, una circuitería del códec 54, un controlador 56 y una memoria 58. Los circuitos individuales y los elementos son todos, excepto para la programación y/o otras instrucciones necesarias para realizar los métodos y procedimientos descritos en este documento, de un tipo conocido en la técnica. En algunas realizaciones, un dispositivo puede incluir menos componentes que todos los mostrados en las Figuras 3 y 4. Por ejemplo, un adaptador u otro componente periférico conectable (por ejemplo, una conexión de Bus Serie Universal) a un ordenador portátil u otro dispositivo puede incluir una antena, una circuitería de la interfaz de radio, un controlador y una memoria, pero pueden faltar la pantalla, el teclado, el micrófono y/o el puerto de infrarrojos.

Ciertas realizaciones descritas en este documento se han descrito en el contexto general de etapas o procesos de métodos, que pueden implementarse en una realización por un producto de programa de ordenador, incorporados en un medio de almacenamiento legible por un ordenador, incluyendo instrucciones ejecutables por un ordenador, tales como el código de programa, ejecutado por uno o más ordenadores en entornos de conexión en red. De forma general, los módulos de programa pueden incluir rutinas, programas, objetos, componentes, estructuras de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Las instrucciones ejecutables por ordenador, las estructuras de datos asociadas, y los módulos de programa representan ejemplos del código de programa para la ejecución de etapas de los procedimientos desvelados en este documento. La secuencia particular de tales instrucciones ejecutables o estructuras de datos asociadas representan ejemplos de los actos correspondientes para la implementación de las funciones descritas en tales etapas o procesos.

Las realizaciones de la presente invención pueden implementarse en software, hardware, lógica de aplicación o una combinación de software, hardware y lógica de aplicación. El software, la lógica de aplicación y/o el hardware pueden residir sobre un conjunto de chips (por ejemplo, uno o más circuitos integrados (IC) o circuitos integrados de aplicación específica (ASIC), un dispositivo móvil, un ordenador de sobremesa, un ordenador portátil, un servidor, un adaptador u otro componente periférico, etc. La lógica de aplicación, el software o un conjunto de instrucciones se mantiene preferiblemente sobre uno cualquiera de los diversos medios convencionales legibles por ordenador. En el contexto de este documento, un "medio legible por ordenador" puede ser cualquier medio o que puede contener, almacenar, comunicar, propagar o transportar las instrucciones para su uso por, o en conexión con, un sistema de ejecución de instrucciones, aparato o dispositivo.

La implementaciones de software y de Web de las diversas realizaciones pueden realizarse con técnicas de programación normalizada con lógica basada en normas y otras lógicas para realizar las diversas etapas o procesos de búsqueda de bases de datos, etapas o procesos de correlación, etapas o procesos de comparación y etapas o procesos de decisión. Debería observarse que las palabras "componente" y "módulo" como se usan en este documento, pretenden incluir las implementaciones usando una o más líneas de código de software, y/o implementaciones de hardware, y/o equipo para la recepción de las entradas manuales.

La Figura 5 es un diagrama de bloques que muestra detalles adicionales de la MME 130 a partir de la Figura 2. La MME 130 incluye uno o más procesadores 202 y una o más memorias 204, memorias que pueden ser volátiles (por ejemplo, una memoria de acceso aleatorio (RAM)), no volátiles (por ejemplo, un controlador de disco magnético) o incluir ambos componentes volátil y no volátil. La MME 130 puede ser un servidor independiente u otro elemento de red, o puede residir dentro de un elemento de red que también realiza otras funciones de red. Las entradas a la MME 130 y las salidas desde la misma a través de las diversas interfaces mostradas (es decir, las interfaces S1-MME, S10, S11, S6a y Gn), así como a través de otras interfaces, pueden estar sobre medios físicos separados. Como alternativa, las comunicaciones sobre múltiples interfaces pueden combinarse sobre una única conexión física (por ejemplo, como paquetes separados sobre una única conexión física de la red IP). El procesador 202 recibe y envía comunicaciones sobre las diversas interfaces mostradas, y comunica con la memoria 204 para recuperar y almacenar datos, de modo que realiza las operaciones de la MME descritas en este documento.

La descripción anterior de las realizaciones se ha presentado con propósitos de ilustración y descripción. La descripción anterior no pretende ser exhaustiva o limitar las realizaciones de la presente invención a la forma precisa desvelada, y son posibles modificaciones y variaciones a la luz de las enseñanzas anteriores o puede adquirirse de la puesta en práctica de las diversas realizaciones. Las realizaciones tratadas en este documento se eligieron y se describieron para explicar los principios y la naturaleza de las diversas realizaciones y su aplicación práctica para posibilitar a un especialista en la técnica utilizar la presente invención en diversas realizaciones y con diversas modificaciones según se adapten al uso particular contemplado. Las características de las realizaciones descritas en este documento pueden combinarse en todas las combinaciones posibles de los procedimientos, aparatos, módulos, sistemas y productos de programa de ordenador.

REIVINDICACIONES

1. Un procedimiento que comprende:

recibir una petición de transferencia de contexto desde una primera entidad de red (140) en una segunda entidad de red (130), incluyendo la petición de transferencia de contexto un campo de información que contiene material de autenticación correspondiente a un dispositivo móvil (100); calcular el material de validación en la segunda entidad de red (130), en el que el material de validación se calcula a partir de información conocida por la segunda entidad de red (130) para ser contenida en el dispositivo móvil (100), y en el que el material de validación no se transfirió anteriormente desde la segunda entidad de red (130) al dispositivo móvil (100); y

determinar si el material de validación coincide con el material de autenticación.

2. El procedimiento de la reivindicación 1, que comprende además:

una vez determinado que el material de validación coincide con el material de autenticación, autenticar la petición de transferencia de contexto y transferir la información de contexto a la primera entidad de red (140).

3. El procedimiento de la reivindicación 1, que comprende además:

una vez determinado que el material de validación no coincide con el material de autenticación, enviar un mensaje de error a la primera entidad de red (140);

posteriormente al envío del mensaje de error, recibir una segunda petición de transferencia de contexto desde la primera entidad de red (140), indicando la segunda petición de transferencia de contexto la autorización del dispositivo móvil (100); y

en respuesta a la segunda petición de transferencia de contexto, transferir la información de contexto a la primera entidad de red (140).

4. El procedimiento de cualquiera de las reivindicaciones 1 a 3, en el que el campo de información comprende un campo de información de la firma del identificador temporal de la estación móvil de la red de paquetes conmutados.

5. El procedimiento de cualquiera de las reivindicaciones 1 a 4, en el que el material de validación se deduce a partir de al menos una clave específica del usuario.

6. El procedimiento de la reivindicación 5, en el que la, al menos una clave específica del usuario es una clave de la entidad de gestión de la seguridad de acceso.

7. El procedimiento de la reivindicación 5, en el que la, al menos una clave específica del usuario se deduce de al menos una clave del estrato no de acceso.

8. El procedimiento de la reivindicación 5, en el que la, al menos una, clave específica del usuario se deduce a partir de al menos una clave de la entidad de gestión de la seguridad de acceso.

9. El procedimiento de cualquiera de las reivindicaciones 1 a 8, en el que el material de autenticación comprende una muestra de tiempo deducida a partir de una clave de la entidad de gestión de la seguridad de acceso.

10. Un medio legible por ordenador para almacenar un programa de ordenador que comprende instrucciones que cuando se ejecutan por un ordenador causan que el ordenador realice cada una de las etapas del procedimiento de la reivindicación 1.

11. El medio legible por ordenador de la reivindicación 10, que comprende instrucciones para realizar el procedimiento de acuerdo con cualquiera de las reivindicaciones de 2 a 9.

12. Un aparato que comprende:

al menos un procesador configurado para

recibir una petición de transferencia de contexto desde una primera red, incluyendo la petición de transferencia de contexto un campo de información que contiene material de autenticación que corresponde a un dispositivo móvil (100),

calcular el material de validación, en el que el material de validación se calcula a partir de información conocida por el aparato a estar contenido en el dispositivo móvil (100), y en el que el material de validación no se transfirió anteriormente desde al aparato al dispositivo móvil (100), y

determinar si el material de validación coincide con el material de autenticación.

13. El aparato de la reivindicación 12, en el que al menos un procesador está configurado para realizar el procedimiento de cualquiera de las reivindicaciones de 2 a 9.

14. Un procedimiento que comprende:

operar un dispositivo móvil (100) dentro de una primera red inalámbrica:

calcular el material de autenticación en el dispositivo móvil (100) en base a información compartida con un elemento de la primera red inalámbrica (130);

transmitir una actualización del área de encaminamiento desde el dispositivo móvil en una segunda red inalámbrica, en el que la segunda red inalámbrica es diferente de la primera red inalámbrica, y en el que la petición de actualización del área de encaminamiento incluye un campo de información que contiene el material de autenticación; y

recibir en el dispositivo móvil, como resultado de la transmisión de la petición de actualización del área de encaminamiento, una aceptación de actualización del área de encaminamiento desde la segunda red inalámbrica.

15. Un medio legible por ordenador para el almacenamiento de un programa de ordenador que comprende instrucciones que cuando se ejecutan por un ordenador causan que el ordenador realice cada una de las etapas del procedimiento de la reivindicación 14.

16. Un aparato que comprende:

al menos un procesador configurado para

operar el aparato dentro de una primera red inalámbrica;

calcular el material de autenticación en base a la información compartida con un elemento de la primera red inalámbrica (130);

transmitir una actualización del área de encaminamiento en una segunda red inalámbrica, en el que la segunda red inalámbrica es diferente de la primera red inalámbrica y en el que la petición de actualización del área de encaminamiento incluye una campo de información que contiene el material de autenticación; y

recibir, como resultado de la transmisión de la petición de actualización del área de encaminamiento, una aceptación de la actualización del área de encaminamiento desde la segunda red inalámbrica.

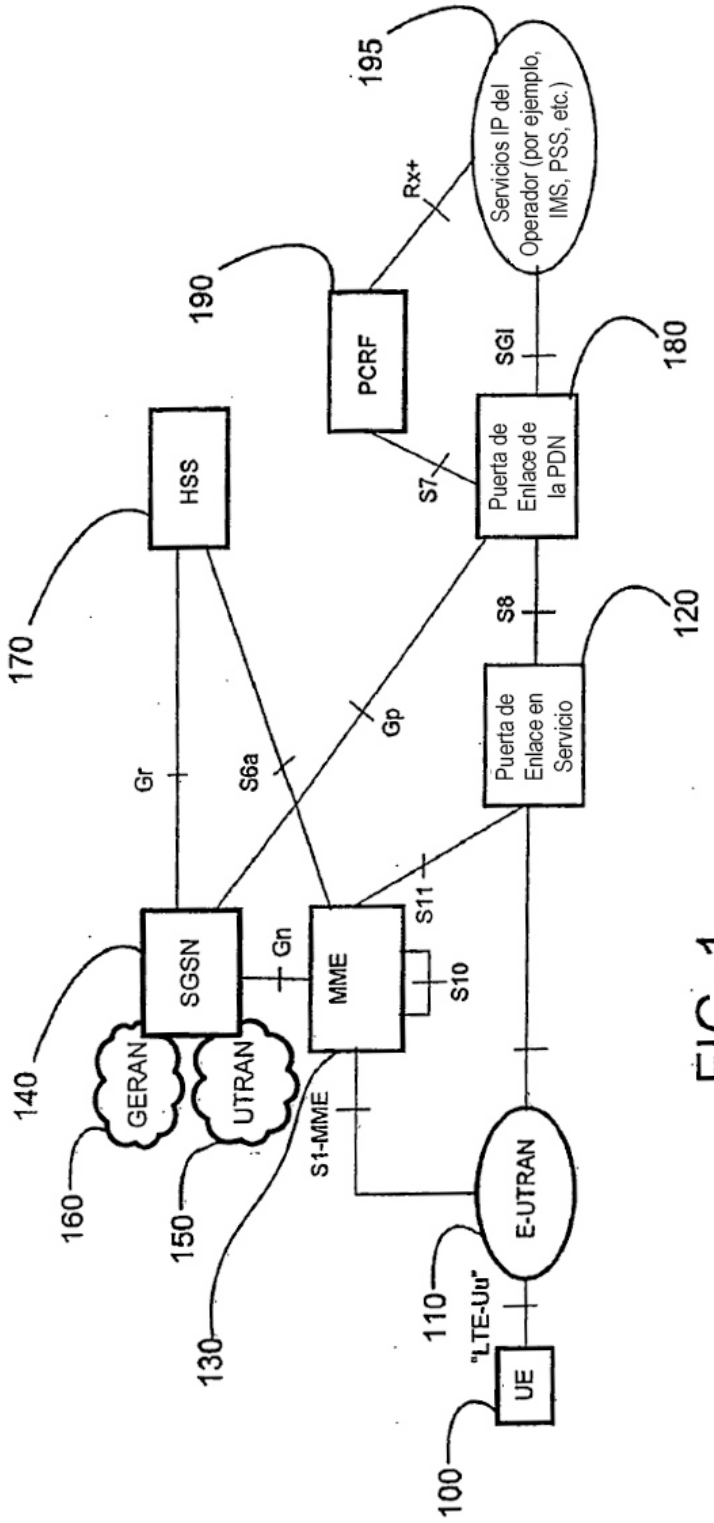
195
Servicios IP del Operador (por ejemplo, IMS, PSS, etc.)
Rx+
190
PCRF
SGi
180
Puerta de Enlace de la PDN
S7
HSS
170
S8
120
Puerta de Enlace en Servicio
Gr
S6a
Gp
S11
Gn
SGSN
MME
S10
140
GERAN
UTRAN
S1-MME
160
150
130
E-UTRAN
110
"LTE-Uu"
UE
100

FIG. 1

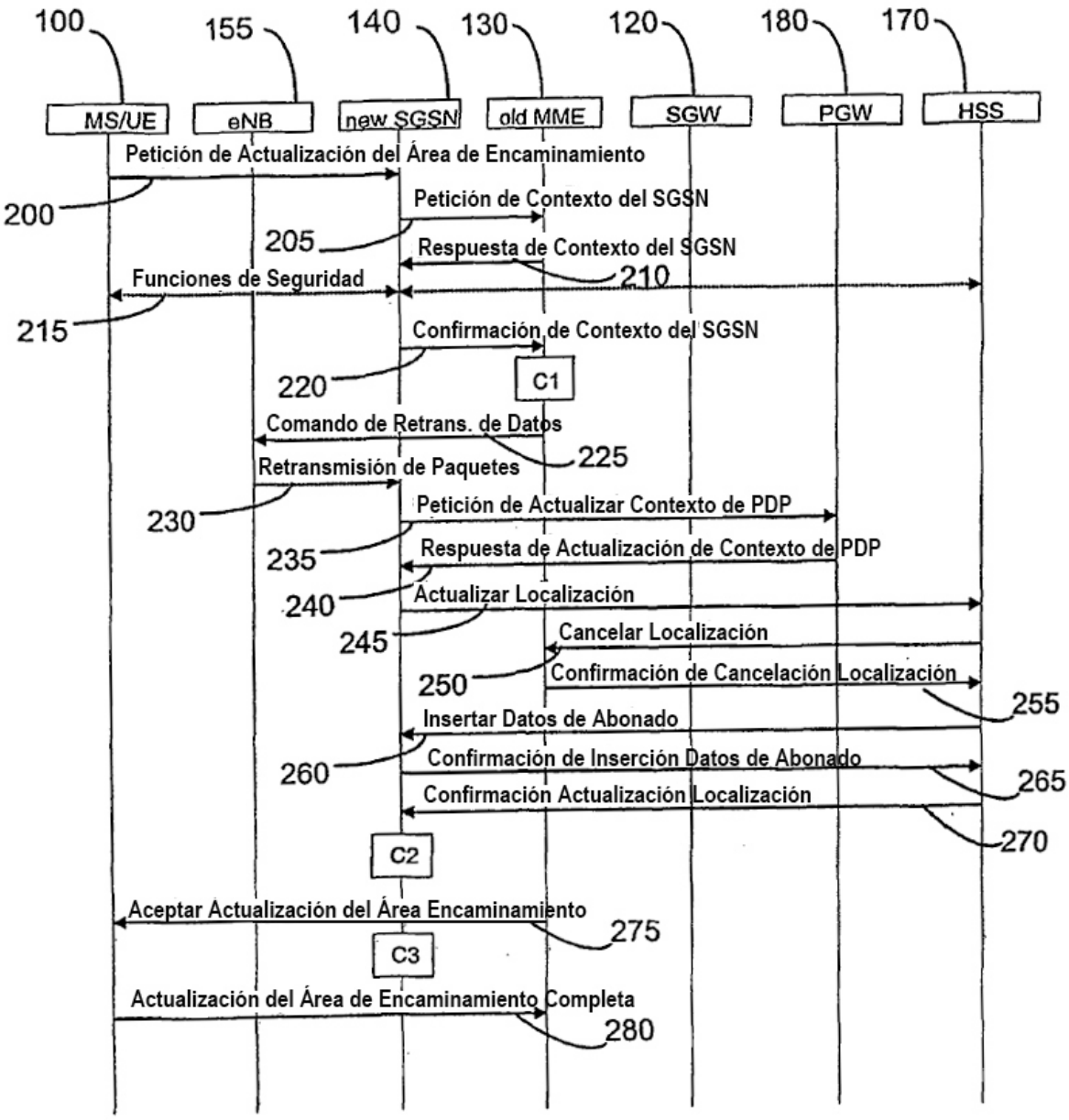
100
155
140
130
120
180
170
MS/UE
eNB
new SGSN
old MME
SGW
PGW
HSS
Petición de Actualización del Área de Encaminamiento
200
Petición de Contexto del SGSN
205
Respuesta de Contexto del SGSN
210
Funciones de Seguridad
215
Confirmación de Contexto del SGSN
220
C1
Comando de Retrans. de Datos
225
Retransmisión de Paquetes
230
Petición de Actualizar Contexto de PDP
235
Respuesta de Actualización de Contexto de PDP
240
Actualizar Localización
245
Cancelar Localización
250
Confirmación de Cancelación Localización
255
Insertar Datos de Abonado
260
Confirmación de Inserción Datos de Abonado
265
Confirmación Actualización Localización
270
C2
Aceptar Actualización del Área Encaminamiento
275
C3
Actualización del Área de Encaminamiento Completa
280

FIG. 2

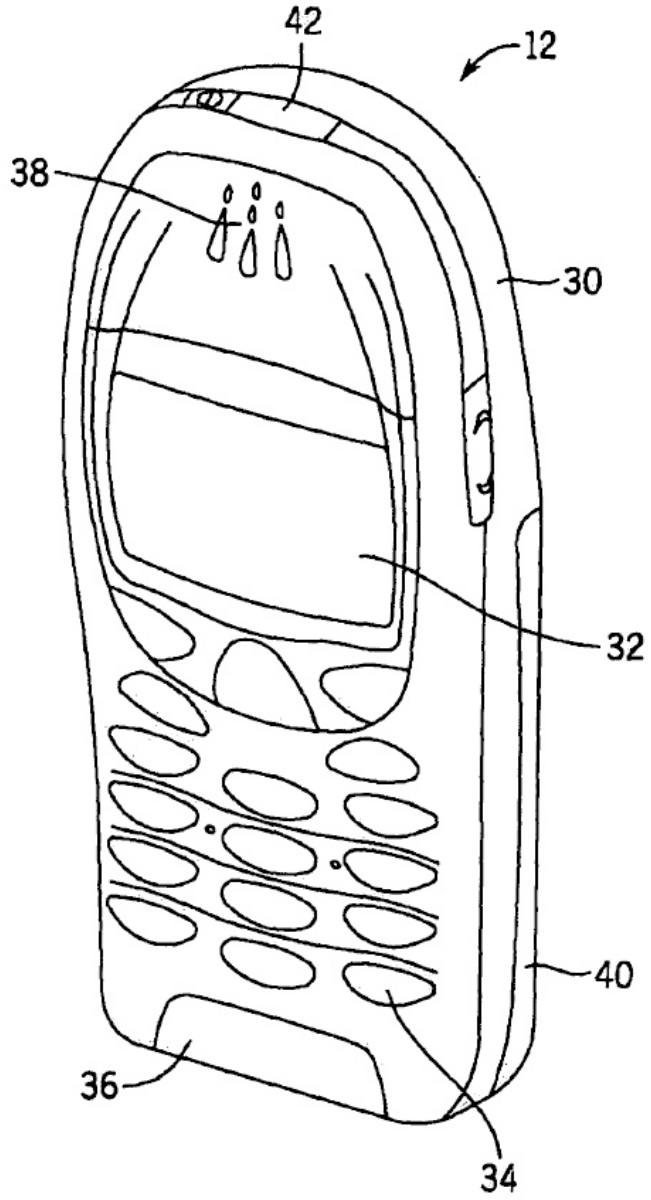

FIG. 3

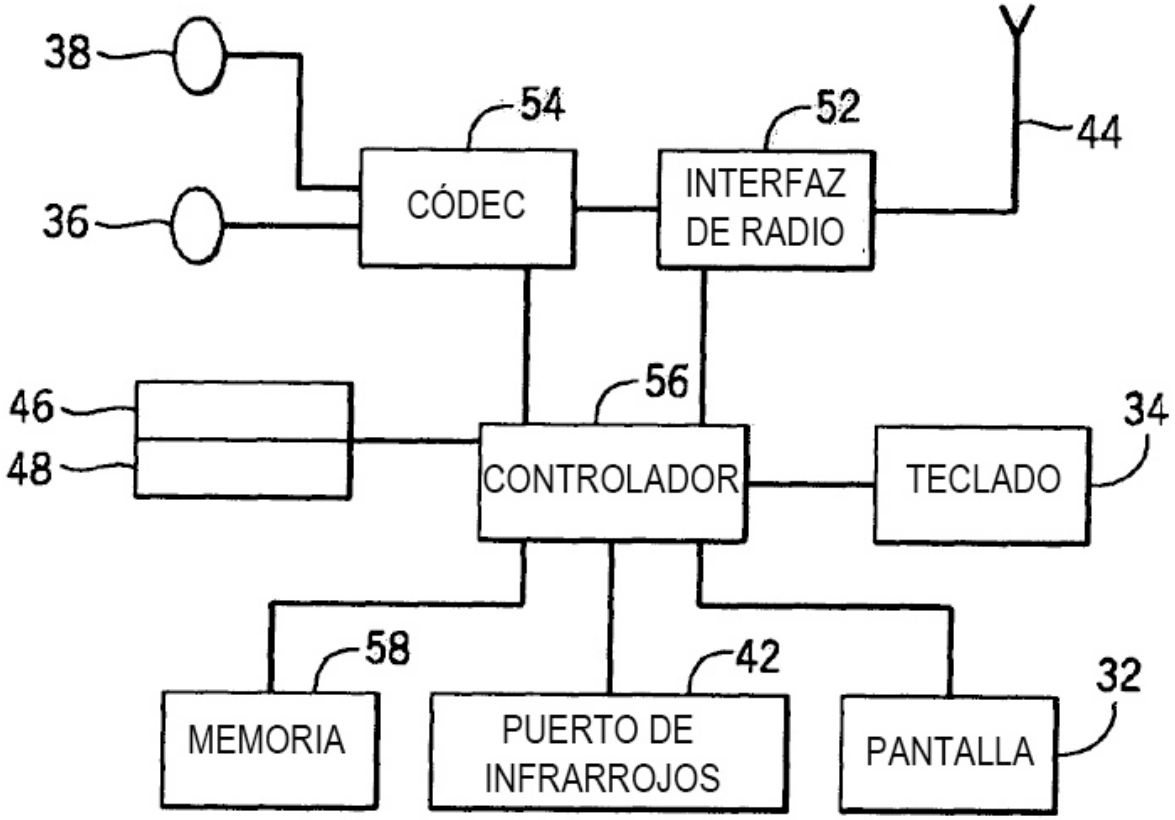
38
36
54
52
44
CÓDEC
INTERFAZ DE RADIO
46
48
56
34
CONTROLADOR
TECLADO
58
42
32
MEMORIA
PUERTO DE INFRARROJOS
PANTALLA

FIG. 4

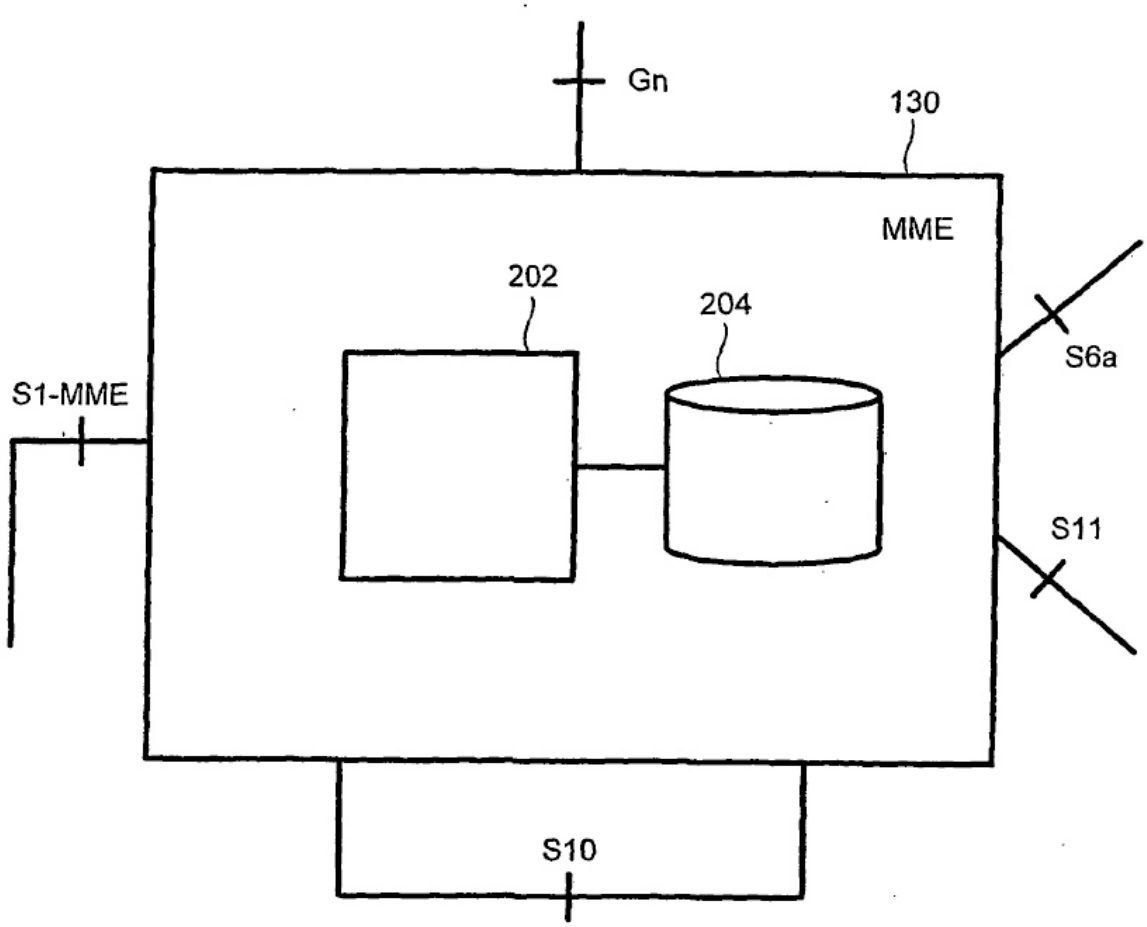

FIG. 5